This document is scheduled to be published in the Federal Register on 06/27/2023 and available online at **federalregister.gov/d/2023-13540**, and on **govinfo.gov**

9111-14-P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. USCBP-2023-0013]

Privacy Act of 1974; System of Records

AGENCY: U.S. Customs and Border Protection, Department of Homeland Security.

ACTION: Notice of a modified system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security (DHS) proposes to modify and reissue a current DHS system of records titled, "DHS/U.S. Customs and Border Protection (CBP)-022 Electronic Visa Update System (EVUS) System of Records." EVUS is an online enrollment system that enables DHS/CBP to collect updated information from certain nonimmigrant visa holders over the length of the visa period that would otherwise not be obtained prior to travel to the United States. DHS/CBP collects this information to determine whether applicants pose a security risk to the United States over the duration of the visa. DHS/CBP is updating this system of records to expand the category of records included in the system. The exemptions for the existing system of records notice will continue to be applicable for this updated system of records notice. This modified system of records notice will be included in the DHS inventory of record systems.

DATES: Submit comments on or before [**INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER**]. This modified system will be effective upon publication. Although this system is effective upon publication, DHS will accept and consider comments from the public and evaluate the need for any revisions to this notice.

ADDRESSES: You may submit comments, identified by docket number USCBP-2023-0013 by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: 202-343-4010.
- Mail: Mason C. Clutter, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528-0655.

Instructions: All submissions received must include the agency name and docket number USCBP-2023-0013. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: Debra L. Danisek, (202) 344-1610, Privacy.CBP@cbp.dhs.gov, CBP Privacy Officer, Privacy and Diversity Office, 1300 Pennsylvania Avenue NW, Washington, D.C. 20229. For privacy questions, please contact: Mason C. Cutter, (202) 343-1717, Privacy@hq.dhs.gov, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528-0655.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, the Department of Homeland Security (DHS) proposes to update and reissue a current Department of Homeland Security system of records titled, "DHS/U.S. Customs and Border Protection (CBP)-022 Electronic Visa Update System (EVUS) System of Records. Upon arrival at a United States port of entry (POE), nonimmigrants[1] are typically required to present a valid passport, a travel and

[1] The term nonimmigrant refers to foreign nationals who are admitted to the United States temporarily for a specific purpose. By contrast, the term immigrant refers to foreign nationals who wish to come to the United States permanently. For additional information about EVUS eligibility, please *see* 81 FR 72491, October 20, 2016.

identity document issued by the traveler's country of citizenship, and valid visa, a document in which an individual applies for that is within the passport signifying that the United States has given the individual permission to enter the country for a specific period. Visa validity periods can vary considerably, and some visas are valid for extended periods of up to ten years, and often for multiple entries.

Frequent travelers to the United States who hold visas with short validity periods must reapply more frequently than those who hold visas with longer validity periods. While visas with a longer validity period provide an opportunity for individuals to travel to the United States with greater ease, it does not allow the U.S. Government to receive regularly updated biographic and other information from repeat visitors who travel to the United States multiple times over the span of the visa.[2] As such, individuals traveling on these visas with longer validity periods are screened using information that is not as recent as for individuals who must obtain visas more frequently. This raises security concerns due to the infrequency in which visa holders may be screened or vetted for threats or inadmissibility.

To alleviate this issue, the DHS/CBP developed EVUS, an online enrollment system that enables DHS/CBP to collect updated information from certain nonimmigrant visa holders prior to travel to the United States without requiring the visa holder to apply for a visa on a more frequent basis.[3] Nonimmigrants enroll in EVUS using an online application. The online application may be completed by either an applicant intending to travel to the United States, or representative on behalf of the traveler (*e.g.,* friend, relative, travel industry professional). The applicant or representative is asked to provide information such as name, date of birth, phone number, email address, passport and visa information, information about current or previous employer, destination address and point

[2] The information updates provided through the visa re-application process include basic biographical and eligibility elements that can change over time (e.g., address, name, employment, criminal history).
[3] *See* Establishment of the Electronic Visa Update System (EVUS) Final Rule, 81 FR 72481 (October 20, 2016).

of contact in the United States, and emergency point of contact information. The applicant or representative also provides responses to eligibility questions regarding communicable diseases, arrests and convictions for certain crimes, history of visa revocation or deportation, and other questions. After the applicant or representative completes all required information, the enrollment may be submitted to DHS/CBP.

Upon receipt, DHS/CBP vets information from the EVUS application against select security and law enforcement databases maintained by DHS, including TECS and the Automated Targeting System (ATS), and other Federal systems. This vetting seeks to identify nonimmigrants who may be inadmissible before they depart for the United States, thereby increasing national security and public safety and reducing traveler delays upon arrival at U.S. ports of entry.

DHS/CBP processes a vast majority of EVUS enrollments within minutes; however, DHS/CBP may take up to 72 hours to approve or deny an enrollment. In addition to providing an approval or denial to the applicant, DHS/CBP also sends a notification to carriers that the individual is enrolled in EVUS and is authorized to board the carrier. A successful EVUS enrollment is generally valid for multiple trips over a period of two years (starting the date that the individual enrolled) or until the individual's passport or visa expires, whichever comes first. This means that if an individual's EVUS enrollment is successful for travel, they do not have to enroll again during the validity period. DHS/CBP continuously vets EVUS enrollment information against new derogatory information received from law enforcement and other national security databases during the course of the individual's enrollment. Therefore, an individual's EVUS status can change at any time.

If an applicant's EVUS enrollment is unsuccessful, DHS/CBP sends a notification that the individual intending to travel should not board the carrier. Alternatively, if an individual does not enroll in EVUS but is required to, DHS/CBP sends a notification to

the carrier notifying them that no EVUS enrollment was found on file and that the carrier is responsible for checking for other valid travel documents that an individual may have.

If a traveler fails to enroll in EVUS when required, their visa will automatically be provisionally revoked. With a provisionally revoked visa, the traveler is not authorized to travel to the United States unless or until they enroll in EVUS and obtains a notification of compliance. If a visa is provisionally revoked due to failure to enroll in EVUS, the individual may attempt to enroll in EVUS. If successful, the provisional revocation will be reversed. In addition, non-compliance with EVUS is a basis for commercial carriers to deny boarding to an individual seeking to travel to the United States. Because non-compliance with EVUS results in automatic provisional revocation of the individual's visa, the individual would not have valid travel documents upon attempting to board.

DHS/CBP is publishing this modified system of records notice to make changes to the underlying system of records and to enhance transparency.

DHS/CBP is expanding the category of records to include social media identifier(s) (*e.g.,* username(s)/handle(s), platform(s) used). This change is consistent with the information collected in Department of State visa application forms.[4] Applicants and representatives have the option, but are not required, to provide social media information and are therefore able to submit the application without including any social media information. A decision to forgo responding to the optional social media question will not result in denial or an "unsuccessful" or "revoked visa" response from EVUS. This collection of information assists DHS/CBP in assessing an individual's eligibility to travel to or be admitted to the United States. DHS/CBP uses the information to search publicly available information on social media platforms. The collection of applicants'

[4] In 2019, the Department of State obtained approval from the Office of Management and Budget (OMB) through the Paperwork Reduction Act (PRA) to collect social media information. The collection of social media information was approved under OMB Control Number 1405-0182 on April 11, 2019.

social media identifiers and associated platforms assists DHS/CBP with more timely visibility of the publicly available information on the platforms provided by the applicant. For example, social media information can provide positive, confirmatory information or support a traveler's EVUS application. Information found on social media may help distinguish individuals of concern from applicants whose information substantiates their eligibility for travel. It can also be used to identify potential deception, fraud, or previously unidentified national security or law enforcement concerns. While DHS/CBP is collecting publicly available information about the applicant and their associates, any information found as part of the vetting process will not be stored in EVUS. DHS/CBP retains information collected from publicly available sources, which may include social media information, as well as other information obtained through the vetting process in other systems of record, including TECS and the Automated Targeting System.

Consistent with DHS's information sharing mission, information stored in the DHS/CBP-022 EVUS system of records may be shared with other DHS Components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, DHS/CBP may share information with appropriate Federal, State, local, Tribal, Territorial, foreign, or international government agencies consistent with the routine uses set forth in this System of Records notice.

This modified system will be included in DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which Federal Government agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to information that is maintained in a "system of records". A "system of records" is a group of any records under the control of an agency from which information is retrieved by the

name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. Additionally, the Judicial Redress Act (JRA) provides covered persons with a statutory right to make requests for access and amendment to covered records, as defined by the Judicial Redress Act, along with judicial review for denials of such requests. In addition, the Judicial Redress Act prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act of 1974.

Below is the description of the DHS/CBP-022 Electronic Visa Update System (EVUS) System of Records.

In accordance with 5 U.S.C. sec. 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

SYSTEM NAME AND NUMBER: Department of Homeland Security (DHS)/U.S. Customs and Border Protection (CBP)-022 Electronic Visa Update System (EVUS).

SECURITY CLASSIFICATION: Unclassified and classified. The unclassified data may be retained on classified networks, but this does not change the nature and character of the data until it is combined with classified information.

SYSTEM LOCATION: Records are maintained at DHS/CBP Headquarters in Washington, D.C., and in field offices. Records are replicated from the operational system and maintained on the DHS unclassified and classified networks to allow for analysis and vetting consistent with the stated uses, purposes, and routine uses published in this notice.

SYSTEM MANAGER(S): Director, EVUS Program Management Office, evus@cbp.dhs.gov, U.S. Customs and Border Protection Headquarters, 1300 Pennsylvania Avenue NW, Washington, D.C. 20229.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title IV of the Homeland Security Act of 2002, 6 U.S.C. 201 *et seq*., the Immigration and Naturalization Act, as amended, including secs. 103 (8 U.S.C. 1103), 214 (8 U.S.C. 1184), 215 (8 U.S.C. 1185), and 221 (8 U.S.C. 1201) of the Immigration and Nationality Act (INA), and 8 CFR part 2 and 8 CFR part 215; and the Travel Promotion Act of 2009, Pub. L. 111-145, 22 U.S.C. sec. 2131.

PURPOSE(S) OF THE SYSTEM: EVUS provides a mechanism through which DHS/CBP may obtain information updates from nonimmigrants who hold a passport issued by an identified country containing a U.S. nonimmigrant visa of a designated category. EVUS provides for greater efficiencies in the vetting of certain nonimmigrants by allowing DHS/CBP to identify subjects of potential interest before they depart for the United States, thereby increasing security and reducing traveler delays upon arrival at U.S. ports of entry. EVUS aids DHS/CBP in facilitating legitimate travel while also ensuring public safety and national security.

When DHS/CBP imposes a fee for EVUS enrollment, the tracking number associated with the payment information provided to Pay.gov will be stored in the Credit/Debit Card Data System (CDCDS). CDCDS is covered by DHS/CBP-003 Credit/Debit Card Data System (CDCDS), 76 FR 67755, November 2, 2011, and is used to process EVUS and third-party administrator fees and to reconcile issues regarding payment between EVUS, CDCDS, and Pay.gov. Payment information will not be used for vetting purposes and is stored separately from the EVUS enrollment data.

DHS maintains a replica of some or all of the data in EVUS on the unclassified and classified DHS networks to allow for analysis and vetting consistent with the above stated uses, purposes, and this published notice.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Categories of

individuals covered by this system include: (1) nonimmigrants who hold a passport issued by an identified country containing a U.S. nonimmigrant visa of a designated category; and (2) persons, including U.S. citizens and lawful permanent residents, whose information is provided by the applicant in response to EVUS enrollment questions.

CATEGORIES OF RECORDS IN THE SYSTEM: Individuals who hold a passport issued by an identified country containing a U.S. nonimmigrant visa of a designated category to obtain the required travel authorization by electronically submitting an enrollment consisting of biographic and other data elements via the EVUS website. The categories of records in EVUS include:

- Full name (first, middle, and last);
- Other names or aliases, if available;
- Date of birth;
- City and country of birth;
- Gender;
- Email address;
- Social media identifiers, such as usernames(s) and platform(s) used, if voluntarily provided;
- Telephone number (home, mobile, work, other);
- Home address (address, apartment number, city, State/region);
- Internet protocol (IP) address from which the EVUS application was submitted;[5]
- EVUS enrollment number;
- Global Entry Program Number;
- Country of residence;

[5] EVUS collects the IP address to assist CBP in determining which applicants are eligible to enroll in EVUS. The IP address will be used with the other EVUS application information for vetting, targeting, and law enforcement purposes in ATS. CBP uses the same security and control measures to protect the IP address as it uses for the rest of the application data.

- Passport number;
- Passport issuing country;
- Passport issuance date;
- Passport expiration date;
- Department of Treasury Pay.gov payment tracking number (*i.e.,* confirmation of payment; absence of payment confirmation will result in a "not cleared" determination);
- Country of citizenship;
- Other citizenship (country, passport number);
- National identification number, if available;
- Address while visiting the United States (number, street, city, State);
- Emergency point of contact information (name, telephone number, email address);
- U.S. point of contact (name, address, telephone number);
- Parents' names;
- Current job title;
- Current or previous employer name;
- Current or previous employer street address; and
- Current or previous employer telephone number.

The categories of records in EVUS also include responses to the following questions:

- History of mental or physical disorders, drug abuse or addiction,[6] and current communicable diseases, fevers, and respiratory illnesses;

[6] Immigration and Nationality Act (INA) 212(a)(1)(A). Pursuant to INA 212(a), individuals may be inadmissible to the United States if they have a physical or mental disorder and behavior associated with the disorder that may pose, or has posed, a threat to the property, safety, or welfare of the individual or others, or have had a physical or mental disorder and a history of behavior associated with the disorder, which behavior has posed a threat to the property, safety, or welfare of the individual or others and which behavior is likely to recur or to lead to other harmful behavior, or are determined (in accordance with regulations prescribed by the Secretary of Health and Human Services) to be a drug abuser or addict.

- Past arrests, criminal convictions, or illegal drug violations;
- Previous engagement in terrorist activities, espionage, sabotage, or genocide;
- History of fraud or misrepresentation;
- Previous unauthorized employment in the United States;
- Past denial of visa, or refusal or withdrawal of application for admission at a U.S. port of entry;
- Previous overstay of authorized admission period in the United States;
- Travel history and information relating to prior travel to or presence in Iraq or Syria, a country designated as a state sponsor of terrorism, or another country or area of concern to determine whether travel to the United States poses a law enforcement or security risk; and,
- Citizenship and nationality information, with additional detail required for nationals of certain identified countries of concern.

RECORD SOURCE CATEGORIES: Records are obtained from applicants and representatives (*e.g.,* friend, relative, travel industry professional) through the online EVUS enrollment at https://www.cbp.gov/EVUS. The passport and visa information provided by the applicant and/or representative is originally derived from the U.S. Department of State.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. sec. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. sec. 552a(b)(3) as follows:

A. To the Department of Justice (DOJ), including the U.S. Attorneys Offices, or other Federal agency conducting litigation or proceedings before any court, adjudicative,

or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;

2. Any employee or former employee of DHS in their official capacity;

3. Any employee or former employee of DHS in their individual capacity, only when DOJ or DHS has agreed to represent the employee; or

4. The United States or any agency thereof.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration (NARA) or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. sec. 2904 and 2906.

D. To an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when (1) DHS suspects or has confirmed that there has been a breach of the system of records; (2) DHS has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DHS (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

F. To another Federal agency or Federal entity, when DHS determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing,

minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

G. To an appropriate Federal, State, Tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where CBP believes the information would assist enforcement of applicable civil or criminal laws and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

I. To appropriate Federal, State, local, Tribal, or foreign governmental agencies or multilateral governmental organizations, with the approval of the Chief Privacy Officer, when DHS is aware of a need to use relevant data, that relate to the purpose(s) stated in this System of Records notice, for purposes of testing new technology.

J. To appropriate Federal, State, local, Tribal, or foreign governmental agencies or multilateral governmental organizations for the purpose of protecting the vital health interests of a data subject or other persons (*e.g.,* to assist such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease or to combat other significant public health threats; appropriate notice will be provided of any identified health threat or risk).

K. To third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation, provided disclosure is appropriate in the proper performance of the official duties of the officer making the disclosure.

L. To a Federal, State, Tribal, local, international, or foreign government agency or entity for the purpose of consulting with that agency or entity: (1) to assist in making a determination regarding redress for an individual in connection to a program; (2) for the purpose of verifying the identity of an individual seeking redress in connection with the operations of a DHS Component or program; or (3) for the purpose of verifying the accuracy of information submitted by an individual who has requested such redress on behalf of another individual.

M. To a Federal, State, Tribal, local, international, or foreign government agency or entity in order to provide relevant information related to intelligence or counterterrorism activities authorized by U.S. law, Executive Order, or other applicable national security directives.

N. To the Department of State in the processing of petitions or applications for benefits under the Immigration and Nationality Act, and all other immigration and nationality laws including treaties and reciprocal agreements.

O. To an organization or individual in either the public or private sector, either foreign or domestic, when there is a reason to believe that the recipient is or could become the target of a particular terrorist activity or conspiracy, to the extent the information is relevant to the protection of life or property.

P. To the carrier transporting an individual to the United States, prior to travel, in response to a request from the carrier, to verify an individual's travel authorization status.

Q. To the Department of Treasury's Pay.gov, for payment processing and payment reconciliation purposes.

R. To a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations, or in connection with criminal law proceedings.

S. To a Federal, State, local agency, Tribal, Territorial, or other appropriate entity or individual, through established liaison channels to selected foreign governments, in order to provide intelligence, counterintelligence, or other information for the purposes of intelligence, counterintelligence, or antiterrorism activities authorized by U.S. law, Executive Order, or other applicable national security directive.

T. To a Federal, State, local, Tribal, Territorial, or other foreign government agency or organization, or international organization, lawfully engaged in collecting law enforcement intelligence information, whether civil or criminal, or charged with investigating, prosecuting, enforcing or implementing civil or criminal laws, related rules, regulations or orders, to enable these entities to carry out their law enforcement responsibilities, including the collection of law enforcement intelligence.

U. To the Department of Treasury's Office of Foreign Assets Control (OFAC) for inclusion on the publicly issued List of Specially Designated Nationals and Blocked Persons (SDN List) of individuals and entities whose property and interests in property are blocked or otherwise affected by one or more OFAC economic sanctions programs, as well as information identifying certain property of individuals and entities subject to OFAC economic sanctions programs.

V. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the

disclosure of the information, when disclosure is necessary to preserve confidence in the integrity of DHS, or when disclosure is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent the Chief Privacy Officer determines that release of the specific information in the context of a particular case would constitute a clearly unwarranted invasion of personal privacy.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: DHS/CBP stores records in this system electronically or on paper in secure facilities in a locked drawer behind a locked door. The records are safeguarded with passwords and encryption and may be stored on magnetic disc, tape, and digital media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: DHS/CBP may retrieve records by any of the data elements supplied by the applicant/representative.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Enrollment information submitted to EVUS is retained for 15 years. DHS/CBP ingests EVUS enrollment data into other DHS/CBP systems for vetting purposes and is stored in accordance with the other systems' respective retention periods. For example, EVUS is ingested into the Automated Targeting System and is retained for 15 years and is also ingested into TECS where it is retained for 75 years, consistent with those systems' retention schedules. These retention periods are based on DHS/CBP's historical encounters with suspected terrorists and other criminals, as well as the broader expertise of the law enforcement and intelligence communities. Travel records, including historical records, are essential in assisting DHS/CBP officers with their risk-based assessment of travel indicators and identifying potential links between known and previously unidentified terrorist facilitators. Analyzing these records for these purposes allows DHS/CBP to continue to effectively identify suspect travel patterns and irregularities. If the record is linked to active law enforcement lookout records, DHS/CBP matches to enforcement activities, and/or investigations or cases (*i.e.*, specific and

credible threats; flights, travelers, and routes of concern; or other defined sets of circumstances), the record will remain accessible for the life of the law enforcement matter to support that activity and other enforcement activities that may become related.

Records replicated on the unclassified and classified networks will follow the same retention schedule.

Payment information will not be stored in EVUS but will be forwarded to Pay.gov and stored in CBP's financial processing system, pursuant to the DHS/CBP-003 Credit/Debit Card Data System of Records notice, 76 FR 67755, November 2, 2011. When a traveler's EVUS data is used for purposes of processing their application for admission to the United States, the EVUS data will be used to create a corresponding admission record that is covered in the DHS/CBP-016 Non-Immigrant Information System (NIIS) System of Records notice, 80 FR 13398, March 13, 2015. This corresponding admission record will be retained in accordance with the NIIS retention schedule, which is 75 years.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: DHS/CBP safeguards records in this system according to applicable rules and policies, including all applicable DHS automated systems security and access policies. DHS/CBP has imposed strict controls to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

RECORD ACCESS PROCEDURES: Applicants may access their EVUS information to view and amend their enrollment by providing their EVUS enrollment number and/or name, date of birth, and visa/passport number through the EVUS website. EVUS applicants have the ability to view their EVUS status (successful enrollment,

unsuccessful enrollment, pending) and submit limited updates to their travel itinerary information.

In addition, EVUS applicants and other individuals whose information is included on EVUS enrollment may submit requests and receive information maintained in this system as it relates to data submitted by or on behalf of a person who travels to the United States and crosses the border, as well as, for EVUS applicants, the resulting determination (successful enrollment, pending, unsuccessful enrollment). However, the Secretary of Homeland Security has exempted portions of this system from certain provisions of the Privacy Act of 1974 related to providing the accounting of disclosures to individuals because it is a law enforcement system. DHS/CBP will consider individual requests to determine whether information may be released. In processing requests for access to information in this system, DHS/CBP will review not only the records in the operational system but also the records that were replicated on the unclassified and classified networks and based on this notice provide appropriate access to the information.

Individuals seeking access to and notification of any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Chief Privacy Officer and Headquarters Freedom of Information Act (FOIA) Officer, whose contact information can be found at http://www.dhs.gov/foia under "Contact Information." If an individual believes more than one component maintains Privacy Act records concerning them, the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, Department of Homeland Security, Washington, D.C. 20528-0655, or electronically at https://www.dhs.gov/freedom-information-act-foia. Even if neither the Privacy Act nor the Judicial Redress Act provide a right of access, certain records about you may be available under the Freedom of Information Act.

When an individual is seeking records about themself from this system of records or any other Departmental system of records, the individual's request must conform with the Privacy Act regulations set forth in 6 CFR part 5. The individual must first verify their identity, meaning that the individual must provide their full name, current address, and date and place of birth. The individual must sign the request, and the individual's signature must either be notarized or submitted under 28 U.S.C. sec. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. An individual may obtain more information about this process at http://www.dhs.gov/foia or 1-866-431-0486. In addition, the individual should:

- Explain why they believe the Department would have information being requested;
- Identify which component(s) of the Department they believe may have the information;
- Specify when the individual believes the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records.

If an individual's request is seeking records pertaining to another living individual, the first individual must include a statement from that individual certifying their agreement for the first individual to access their records.

Without the above information, the component(s) may not be able to conduct an effective search, and the individual's request may be denied due to lack of specificity or lack of compliance with applicable regulations.

CONTESTING RECORD PROCEDURES: See "Record Access Procedures" above.

NOTIFICATION PROCEDURES: See "Record Access Procedures" above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: Pursuant to 6 CFR part 5, appendix C, law enforcement and other derogatory information covered in this system is

exempt from 5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G) through (I), (e)(5), and (8); (f); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, pursuant to 5 U.S.C. 552a (k)(1) and (k)(2): 5 U.S.C. 552a(c)(3); (d)(1), (d)(2), (d)(3), and (d)(4); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f).

Despite the exemptions taken on this system of records, DHS/CBP is not taking any exemption from subsection (d) with respect to information maintained in the system as it relates to data submitted by or on behalf of a person who travels to visit the United States and crosses the border, nor shall an exemption be asserted with respect to the resulting determination (authorized to travel, pending, or not authorized to travel). However, pursuant to 5 U.S.C. sec. 552a(j)(2), DHS/CBP plans to exempt such information in this system from sections (c)(3), (e)(8), and (g) of the Privacy Act of 1974, as amended, as is necessary and appropriate to protect this information. Further, DHS will claim exemption from sec. (c)(3) of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. sec. 552a(k)(2) as is necessary and appropriate to protect this information. CBP will not disclose the fact that a law enforcement or intelligence agency has sought particular records because it may affect ongoing law enforcement activities.

When this system receives a record from another system exempted in that source system under 5 U.S.C. sec. 552a(j) or (k), DHS/CBP will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claim any additional exemptions set forth here. For instance, as part of the vetting process, this system may incorporate records from DHS/CBP's Automated Targeting System, and all exemptions for DHS/CBP's Automated Targeting System of Records notice, described and referenced herein, carry forward and will be claimed by DHS/CBP.

HISTORY: 84 FR 30751 (June 27, 2019); 81 FR 60371 (September 1, 2016).

****

Mason C. Clutter,
Chief Privacy Officer,
Department of Homeland Security.
[FR Doc. 2023-13540 Filed: 6/26/2023 8:45 am; Publication Date: 6/27/2023]